FORM PTO-1390 (REV. 11-2000) U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY 'S DOCKET NUMBER: 520.1007

U S APPLICATION NO (If known, see 37 CFR 1 5): 10/049385

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP00/06510	10 July 2000	12 August 1999

TITLE OF INVENTION: METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS

APPLICANT(S) FOR DO/EO/US: Tobias MARTIN et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. [X] The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [X] is attached hereto (required only if not communicated by the International Bureau).
   b. [X] has been communicated by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [X] An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. [X] is attached hereto.
   b. [ ] has been previously submitted under 35 U.S.C. 154(d)(4).
7. [X] Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are attached hereto (required only if not communicated by the International Bureau).
   b. [ ] have been communicated by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [X] have not been made and will not be made.
8. [ ] An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. [X] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [ ] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [X] A FIRST preliminary amendment.
14. [ ] A SECOND or SUBSEQUENT preliminary amendment.
15. [ ] A substitute specification.
16. [ ] A change of power of attorney and/or address letter.
17. [ ] A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. [ ] A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. [ ] A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. [X] Other items or information:
    - Drawing for Prelim. Amendm. (Fig. 1)
    - References cited in Information Disclosure Statement
    - Letter re: Priority

U.S. APPLICATION NO (If known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
10/049385	PCT/EP00/06510	520.1007

21. [X] The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):

	CALCULATIONS PTO USE ONLY
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$860.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**	
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**	
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**	
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 890.00
Surcharge of **$130.00** for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total claims	13 - 20 =	0	x **$18.00**	$
Independent claims	2 - 3 =	0	x **$80.00**	$
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$270.00**	$
TOTAL OF ABOVE CALCULATIONS =				$ 890.00
[ ] Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2. +				$
SUBTOTAL =				$ 890.00
Processing fee of **$130.00** for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				$
TOTAL NATIONAL FEE =				$ 890.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$
TOTAL FEES ENCLOSED =				$ 890.00
			Amount to be refunded:	$
			charged:	$

a. [X] A check in the amount of $ 890.00 to cover the above fees is enclosed.

b. [ ] Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-0552 . A duplicate copy of this sheet is enclosed.

d. [ ] Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO

William C. Gehris, Esq.
Davidson, Davidson & Kappel, LLC
485 Seventh Avenue, 14th Floor
New York, New York 10018
U.S.A.

SIGNATURE

William C. Gehris
NAME

38,156
REGISTRATION NUMBER

[520.1007]

UNITED STATES PATENT AND TRADEMARK OFFICE

Re:	Application of:	Tobias MARTIN et al.
	Serial No.:	To Be Assigned
	International Application No.:	PCT/EP00/06510
	Filed:	Herewith
	For:	METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS

BOX PCT
Asst. Commissioner for Patents
Washington, D.C. 20231

February 11, 2002

PRELIMINARY AMENDMENT

Sir:

Applicants request that the following Amendments be made in the above-identified matter prior to examination thereof:

IN THE DRAWINGS

Please add new Fig. 1 as submitted herewith.

IN THE SPECIFICATION

Before paragraph [0001], please change the heading "Specification" to --BACKGROUND--.

Please amend paragraph [0001] as follows:

[0001] The present invention relates to a method for establishing a common key within a group of subscribers using a publicly known mathematical group and a publicly known element of the group.

Please amend paragraph [0005] as follows:

[0005] A difficulty of the DH-key exchange lies in that Alice does not know whether she actually communicates with Bob or with a cheater. In the IPSec-Standards of the Internet Engineering Task Force (IETF RFC 2412: The OAKLEY Key Determination Protocol), this problem is solved by using public key certificates in which the identity of a subscriber is combined with a public key by a trust center. In this manner, the identity of an interlocutor becomes verifiable.

Page 3, please insert paragraphs [0011.1] and [0011.2] as follows:

--[0011.1] Known from Menezes et al: "Handbook of applied cryptography" 1997 CRC Press. Boca Raton (US) XP002152150 is a method for establishing a common key involving at least three subscribers. In this design approach, a group member (chair) is defined from whom all activities originate. The selection of common key K lies solely with the chair. Subsequently, common key K is sent from the chair to every group member on the basis of the Diffie-Hellman keys determined in pairs, respectively. Thus, common key K is always just as good as it has been selected by the chair.

[0011.2] In Lennon R E et Al: "Cryptographic key distribution using composite keys" Birmingham, Alabama, DEC.3-6, 1978, New York. IEEE, US Vol. CONF. 1978, December 3rd, 1978 (1978-12-03), pp. 26101-26116-6. XP002098158, a key exchange method is described which is limited to two subscribers. In this design approach, each subscriber generates his/her own random number and sends it to the other subscriber in encrypted form. The common key is then determined by each subscriber from the own random number and the encrypted random number received from the other subscriber, using a symmetrical function (EXC-OR).--.

Page 4, before paragraph [0014] please insert the heading --SUMMARY OF THE INVENTION--.

Please amend paragraph [0014] as follows:

[0014] An object of the present invention is to provide a method for generating a common key within a group of at least three subscribers. The intention is for the method to be designed in such a manner that it stands out over the known methods by a small computational outlay and a small communication requirement (few rounds even in the case of many subscribers). At the same time, however, it is intended to have a comparable security standard as the DH method. The method has to be easy to implement. Information on the structure of the group should not be required for carrying out the method.

Page 4, please insert paragraph [0014.1] as follows:

--[0014.1] The present invention provides a method for establishing a common key for a group of at least three subscribers. The method comprises:

generating by each subscriber Ti of the at least three subscribers a respective message Ni = (g^{zi} mod p) from a publicly known element g of large order of a publicly known mathematical group G and a respective random number zi and sending the respective message from the respective subscriber to all other subscribers Tj of the at least three subscribers, each respective random number zi being selected or generated by the respective subscriber Ti;

generating by each subscriber Ti a transmission key k^{ij} from the messages Nj received from the other subscribers Tj, $j \neq i$, and the respective random number zi according to k^{ij}: = Nj^{zi} = $(g^{zj})^{zi}$;

sending by each subscriber Ti the respective random number zi in encrypted form to all other subscribers Tj by generating the message Mij according to Mij := $E(k^{ij}, zi)$, $E(k^{ij}, zi)$ being a symmetrical encryption algorithm in which the data record zi is encrypted with the transmission key k^{ij}; and

determining a common key k by each subscriber Ti using the respective random number zi and the random numbers zj, $j \neq i$, received from the other subscribers according to

$$k: = f(z1, ..., zn),$$

f being a symmetrical function which is invariant under a permutation of its arguments.--.

Before paragraph [0022], please insert the following: the heading --BRIEF DESCRIPTION OF THE DRAWING--; paragraph [0021.1] as follows:

--[0021.1] Fig. 1 shows a flow chart of a method for establishing a common key within a group of subscribers.--;

the heading --DETAILED DESCRIPTION--; and paragraph [0021.2] as follows:

[0021.2] Referring to Fig. 1, in a method according to the present invention for establishing a common key within a group of subscribers, by each subscriber Ti of the at least three subscribers a respective message $Ni = (g^{zi} \bmod p)$ is generated from a publicly known element g of large order of a publicly known mathematical group G and a respective random number zi and the respective message is sent from the respective subscriber to all other subscribers Tj of the at least three subscribers (see block 102). Each respective random number zi is selected or generated by the respective subscriber Ti. Then, by each subscriber Ti a transmission key k^{ij} is generated from the messages Nj received from the other subscribers Tj, $j \neq i$, and the respective random number zi according to $k^{ij} := Nj^{zi} = (g^{zj})^{zi}$ (see block 104). By each subscriber Ti the respective random number zi is sent in encrypted form to all other subscribers Tj by generating the message Mij according to $Mij := E(k^{ij}, zi)$, $E(k^{ij}, zi)$ being a symmetrical encryption algorithm in which the data record zi is encrypted with the transmission key k^{ij} (see block 106). Finally, a common key k is determined by each subscriber Ti using the respective random number zi and the random numbers zj, $j \neq i$, received from the other subscribers according to $k := f(z1, ..., zn)$, f being a symmetrical function which is invariant under a permutation of its arguments (see block 108).--.

Please amend paragraph [0026] as follows:

[0026] A variant of the method is to assign a special role to one of subscribers T1-Tn for the execution of the second method step. If this role is assigned, for example, to subscriber T1, then method steps 2 and 3 or b and c are executed only by subscriber T1. In fourth method step d, all subscribers T1-Tn involved in the method compute common key k according to the assignment $k := h(z1, g^{z2}, ..., g^{zn})$, it being required for (x1, x2, ..., xn) to be a function which is symmetrical in arguments x2, ... xn. This variant drastically reduces the number of messages to be sent. An example of such a function g is, for instance,

$$k := h(z1, g^{z2}, ..., g^{zn}) = g^{z1\,z1} \cdot g^{z2 \cdot z1} \ldots g^{zn\,z1}.$$

Page 9, please delete the heading "METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS".

Page 9, first line change "(2) What is claimed is" to --WHAT IS CLAIMED IS--.

IN THE CLAIMS:

Please cancel claim1 as presented in the underlying International Application No. PCT/EP00/06510 and cancel revised claims 1-2 annexed to the International Preliminary Examination Report, and add new claims 3-6 as follows:

--3. (new) A method for establishing a common key for a group of at least three subscribers, the method comprising:

generating by each subscriber Ti of the at least three subscribers a respective message Ni = (g^{zi} mod p) from a publicly known element g of large order of a publicly known mathematical group G and a respective random number zi and sending the respective message from the respective subscriber to all other subscribers Tj of the at least three subscribers, each respective random number zi being selected or generated by the respective subscriber Ti;

generating by each subscriber Ti a transmission key k^{ij} from the messages Nj received from the other subscribers Tj, $j \neq i$, and the respective random number zi according to k^{ij}: = Nj^{zi} = $(g^{zj})^{zi}$;

sending by each subscriber Ti the respective random number zi in encrypted form to all other subscribers Tj by generating the message Mij according to Mij := $E(k^{ij}, zi)$, $E(k^{ij}, zi)$ being a symmetrical encryption algorithm in which the data record zi is encrypted with the transmission key k^{ij}; and

determining a common key k by each subscriber Ti using the respective random number zi and the random numbers zj, $j \neq i$, received from the other subscribers according to

$$k: = f(z1, ..., zn),$$

f being a symmetrical function which is invariant under a permutation of its arguments.

4. (new) The method as recited in claim 3 wherein the transmission key k^{ij} is known to subscriber Tj according to $k^{ij} = k^{ji}$.

5. (new) A method for establishing a common key for a group of at least three subscribers, the method comprising:

generating by each subscriber a respective message Ni = (g^{zi} mod p) from a publicly

known element g of large order of a publicly known mathematical group G and a respective random number zi and sending the respective message by each subscriber except a predetermined first subscriber T1 of the at least three subscribers to the first subscriber T1, each respective random number zi being selected or generated by the respective subscriber Ti;

encrypting by the first subscriber T1 the received messages Nj of the other subscribers Tj, $j \neq 1$, with the random number z1 to form a respective transmission key k^{1j} for each subscriber Tj;

sending by the first subscriber T1 the random number z1 to all other subscribers Tj in encrypted form by generating a message M1j according to $M1j := E(k^{1j}, z1)$, $E(k^{1j}, z1)$ being a symmetrical encryption algorithm in which the random number z1 is encrypted with the transmission key k^{1j}; and

determining a common key k by each subscriber Ti using the values Ni and Nj, $j \neq i$, and the random number z1 sent by the first subscriber T1 in encrypted form using

$$k: = h\,(z1, g^{z2}, ..., g^{zn}),$$

h (x1, x2, ..., xn) being a function which is symmetrical in the arguments x2, ..., xn.

6. (new) The method as recited in claim 5 wherein the key is known to subscriber Tj according to $k^{1j} = k^{j1}$.--.

IN THE ABSTRACT:

Please replace the abstract of record with the new abstract submitted herewith as a separate sheet.

REMARKS

New Fig. 1 is submitted herewith for the Examiner's consideration. The application has been amended to place the application in proper format and correct errors. It is respectfully submitted that the claims have not been narrowed. It is respectfully submitted that no new matter has been added.

Applicants believe that no fees are due as a result of this amendment. In the event of a fee discrepancy, please charge our Deposit Account No. 50-0552.

Respectfully submitted,

DAVIDSON, DAVIDSON & KAPPEL, LLC

By: _____

William C. Gehris
Reg. No. 38,156

Davidson, Davidson & Kappel, LLC
485 Seventh Avenue - 14th Floor
New York, New York 10018
(212) 736-1940

"Express Mail" mailing label no EL 914449536 US
Date of deposit February 11, 2002
I hereby certify that this correspondence and/or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231"

DAVIDSON, DAVIDSON & KAPPEL, LLC

BY: _____
Samuel Gomez

Abstract

A method for establishing a common key for a group of at least three subscribers includes using a publicly known mathematical number group and a higher order element of the group $g \in G$. In the first step, a message corresponding to Ni: $= g^{zi}$ mod p is sent by each subscriber to all other subscribers (Tj), (zi) being a random number chosen from the set (1, ..., p-2) by a random number generator. In the second step, each subscriber (Ti) selects a transmission key kij: $= (g^{zj})^{zi}$ for each other subscriber (Tj) from the received message (g^{zj}), with $i \neq j$, for transmitting their random number (zi) to the subscribers (Tj). In the third step, the common key k is calculated as k: = f(z1, z2, ..., zn) for each subscriber Ti.

Application of: Tobias MARTIN et al. [520.1007]
International Application No. PCT/EP00/06510
Filed Herewith

VERSION OF AMENDMENTS
WITH MARKINGS TO SHOW CHANGES MADE

IN THE SPECIFICATION:

Page1, heading before paragraph [0001]: [Specification] --Background--.

Page 1, paragraph [0001]:
[0001] The present invention relates to a method for establishing a common key within a group of subscribers [according to the definition of the species in the independent claim] using a publicly known mathematical group and a publicly known element of the group.

Page 1, paragraph [0005]:
[0005] [The] A difficulty of the DH-key exchange lies in that Alice does not know whether she actually communicates with Bob or with a cheater. In the IPSec-Standards of the Internet Engineering Task Force (IETF RFC 2412: The OAKLEY Key Determination Protocol), this problem is solved by using public key certificates in which the identity of a subscriber is combined with a public key by a trust center. In this manner, the identity of an interlocutor becomes verifiable.

Page 4, paragraph [0014]:
[0014] [The method according to] An object of the present invention [has to be suitable] is to provide a method for generating a common key within a group of at least three subscribers. The intention is for the method to be designed in such a manner that it stands out over the known methods by a small computational outlay and a small communication requirement (few rounds

even in the case of many subscribers). At the same time, however, it is intended to have a comparable security standard as the DH method. The method has to be easy to implement. Information on the structure of the group should not be required for carrying out the method.

Page 6, paragraph [0026]:

[0026] A variant of the method is to assign a special role to one of subscribers T1-Tn for the execution of the second method step. If this role is assigned, for example, to subscriber T1, then method steps 2 and 3 or b and c are executed only by subscriber T1. In fourth method step d, all subscribers T1-Tn involved in the method compute common key k according to the [equation] assignment $k: = h(z1, g^{z2}, ..., g^{zn})$, it being required for (x1, x2, ..., xn) to be a function which is symmetrical in arguments x2, ... xn. This variant drastically reduces the number of messages to be sent. An example of such a function g is, for instance,

$$k: = h(z1, g^{z2}, ..., g^{zn}) = g^{z1\,z1} \cdot g^{z2\,z1} \ldots g^{zn\,z1}.$$

Page 9, heading: [METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS].

Page 9 first line : --WHAT IS CLAIMED IS-- [(2) What is claimed is].

IN THE ABSTRACT:

Please amend the abstract as follows:

[The inventive method is based on] A method for establishing a common key for a group of at least three subscribers includes using a publicly known mathematical number group and a higher order element of the group $g \in G$. In the first [work] step, a message corresponding to $Ni: = g^{zi}$ mod [p)] p is sent by each subscriber to all other subscribers (Tj), (zi) being a random number chosen from the set (1, ..., p-2) by a random number generator. In the second [work] step, each subscriber (Ti) selects a transmission key $kij: = (g^{zj})^{zi}$ for each other subscriber (Tj) from the received message (g^{zj}), with $i \neq j$, for transmitting their random number (zi) to the subscribers (Tj). In the third [work] step, the common key k is calculated as k: = f(z1, z2, ..., zn) for each subscriber Ti.

[520.1007]

METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS

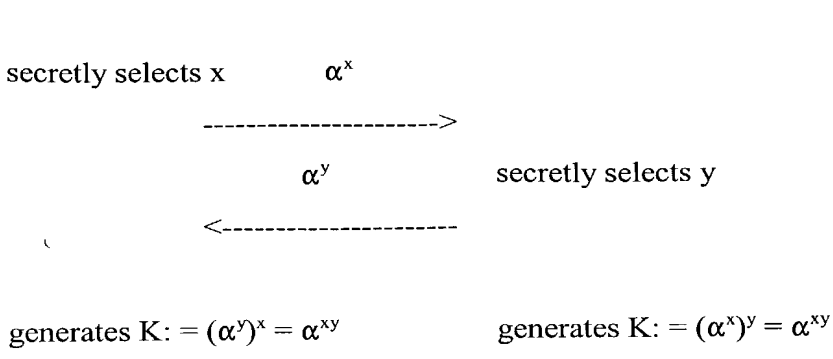
Specification

[0001] The present invention relates to a method for establishing a common key within a group of subscribers according to the definition of the species in the independent claim.

[0002] Encryption methods of varied types belong to state of the art and increasingly have commercial importance. They are used for sending messages over commonly accessible transmission media, but only the owners of a cryptokey being able to read these messages in plain text.

[0003] A known method for establishing a common key over unsecure communication channels is, for example, the method by W. Diffie and W. Hellmann (see DH-Method W. Diffie and M. Hellmann, see New Directions in Cryptography, IEEE Transaction on Information Theory , IT-22(6): 644-654, November 1976).

[0004] The basis of the Diffie Hellmann key exchange (DH-key exchange) is the fact that it is virtually impossible to compute logarithms modulo a large prime number p. In the example depicted below, Alice and Bob make use of this in that they each secretly select a number x or y, respectively, which are smaller than p (and relatively prime to p-1). Then, they (successively or simultaneously) send each other the x^{th} (or y^{th}) power modulo p of a publicly known number α. They are able to compute a common key $K: = \alpha^{xy}$ mod p from the received powers by another exponentiation modulo p with x or y, respectively. An attacker who sees only α^x mod p and α^y mod p cannot compute K therefrom. (The only method for this which is known today would be to initially compute the logarithm, for example, of α^x to base α modulo p, and to subsequently exponentiate α^y therewith.)



Example of the Diffie-Hellmann key exchange

[0005] The difficulty of the DH-key exchange lies in that Alice does not know whether she actually communicates with Bob or with a cheater. In the IPSec-Standards of the Internet Engineering Task Force (IETF RFC 2412: The OAKLEY Key Determination Protocol), this problem is solved by using public key certificates in which the identity of a subscriber is combined with a public key by a trust center. In this manner, the identity of an interlocutor becomes verifiable.

[0006] The DH-key exchange can also be carried out using other mathematical structures, for example, with finite bodies GF (2^n) or elliptical curves. Using these alternatives, it is possible for the performance to be improved. However, this method is only suitable to agree upon a key between two subscribers.

[0007] Several attempts have been made to extend the DH method to three or more subscribers (group DH). An overview of the related art is offered by M. Steiner, G. Tsudik, M. Waidner in Diffie-Hellmann Key Distribution Extended to Group Communication, Proc. 3rd ACM Conference on Computer and Communications Security, March 1996, New Delhi, India.

[0008] An extension of the DH method to subscribers A, B and C is described, for example,

by the following table (the calculation is in each case mod p):

Subscriber A;B;C	A → B	B → C	C → A
1st round	g^a	g^b	g^c
2nd round	g^{ca}	g^{ab}	g^{bc}

[0009] Subsequent to carrying out these two rounds, each of the subscribers is able to compute secrete key g^{abc} mod p.

[0010] Known from Burmester, Desmedt, A secure and efficient conference key distribution system, Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994 is, moreover, a design approach in which two rounds are required for generating the key, it being necessary to send n messages of length p = approx. 1000 bits for n subscribers in the second round.

[0011] Further relevant design approaches are known from M. Burmester and Y. Desmedt, Efficient and secure conference key distribution, Cambridge Workshop on Security Protocols, Springer LNCS 1189, pp 119-129 (1996). However, it is assumed here that secure channels already exist between the subscribers.

[0012] In all of these extensions, at least one of the following problems occurs:

- The subscribers have to be organized in a specific fashion; in the above example, for instance, as a circle, that is, a structure of the subscriber group must previously be known.
- If a central unit is used to coordinate the key agreement, then the subscribers have no influence on the selection of the key with respect to this central unit.
- The number of rounds depends on the number of subscribers.

For the above reasons, these methods are generally difficult to implement and require considerable computational outlay.

[0013] The further development of the DH method to a public key method is known from T. ElGamal "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.", IEEE Transactions on Information Theory, July 1985.

[0014] The method according to the present invention has to be suitable for generating a common key within a group of at least three subscribers. The intention is for the method to be designed in such a manner that it stands out over the known methods by a small computational outlay and a small communication requirement (few rounds even in the case of many subscribers). At the same time, however, it is intended to have a comparable security standard as the DH method. The method has to be easy to implement. Information on the structure of the group should not be required for carrying out the method.

[0015] The method according to the present invention which satisfies this problem definition is based on the same mathematical structures as the DH method and has therefore comparable security features. In comparison with the group DH methods proposed heretofore, however, it is considerably more efficient with regard to the computational outlay and communication requirement.

[0016] In the following, the operating principle of the method will be explained in greater detail. The defined subscribers of the method are denoted by T1-Tn and each individual, not specifically named subscriber is denoted by Ti. All other subscribers involved in the method are denoted by Tj except for the respective subscriber Ti. The publicly known components of the method are a publicly known mathematical group G, preferably the multiplicative group of all integral numbers modulo a large prime number p, and an element g of group G, preferably a number $0 < g < p$ having large multiplicative order. However, it is also possible to use other suitable mathematical structures for group G, for example, the multiplicative group of a finite body or the group of the points of an elliptical curve. In the following, the method will be described on the basis of the group of numbers modulo a prime number p.

[0017] The method is based on four method steps.

In the first method step, a message of the form $Ni = g^{zi} \bmod p$ is generated by each not specifically named subscriber Ti and sent to all other subscribers Tj, zi preferably being a random number from the set {1, ... p-2} selected via a random-number generator.

[0018] In the second method step, each subscriber Ti computes a common transmission key $k^{ij} := (g^{zj})^{zi}$ from received message g^{zj} for each further subscriber Tj, where $i \neq j$. Since $k^{ij} = k^{ij}$ applies, subscribers Ti and Tj now know a common transmission key k^{ij} and can therefore communicate confidentially.

[0019] In the third method step, each subscriber Ti uses transmission key k^{ij} to confidentially send his/her random number zi to the other subscribers Tj, respectively. In the process, the encryption of random number zi with transmission key k^{ij} is carried out using a symmetrical encryption method. This means that, upon completion of the method step, each subscriber Ti knows the encrypted random numbers of all other subscribers Tj in addition to his/her own random number so that the conditions are given for computing a common key k.

[0020] In the fourth method step, common key k is computed according to equation

$k = f(z1, z2, ..., zn)$

at each subscriber Ti, with f being an arbitrary symmetrical function.. In this case, symmetry means that the value of the function remains the same even when arbitrarily exchanging the arguments. Examples of symmetrical functions include

- the multiplication in a (finite) body: $k := z1 \ldots zn$,
- the addition in a (finite) body: $k := z1 + \ldots + zn$,
- the bitwise XOR of zi: $k := z1 \oplus \ldots \oplus zn$,
- the exponentiation of g with zi: $k := g^{z1 \ldots zn}$
- countless further possibilities.

[0021] The transmission of the messages generated in steps 1 and 2 can be carried out both via point-to-point connections and by broadcast or multicast.

[0022] In the following, the method according to the present invention will be explained in greater detail in the light of a concrete example for three subscribers A, B and C. However, the number of subscribers can be extended to an arbitrary number of subscribers.

[0023] In this example, the length of number p is 1024 bits; g has a multiplicative order of at least 2^{160}.

[0024] The method according to the present invention is executed according to the following method steps:

1. Subscriber A sends $Na = g^{za} \bmod p$ to subscribers B and C, subscriber B sends $Nb = g^{zb} \bmod p$ to subscribers A and C, and subscriber C sends $Nc = g^{zc} \bmod p$ to subscribers A and B.
2. Subscriber A computes $kab = Nb^{za} \bmod p$ and $kac = Nc^{za} \bmod p$. Subscribes B and C proceed analogously.
3. Subscriber A sends message Mab = E(kab, za) to subscriber B and message Mac = E(kac, za) to subscriber C. Here, E(k, m) denotes the symmetrical encryption of the data record with algorithm E under transmission key k^{y}. Subscribes B and C proceed analogously.
4. Subscriber A computes common key k according to the function $k = g^{ka \cdot kb \cdot kc}$. Subscribers B and C compute common key k analogously.

[0025] The method described above makes do with the minimum number of two rounds between subscribers A, B and C. The number of rounds required for carrying out the method according to the present invention remains limited to two rounds even with an arbitrary number of subscribers T1-Tn .

[0026] A variant of the method is to assign a special role to one of subscribers T1-Tn for the execution of the second method step. If this role is assigned, for example, to subscriber T1, then method steps 2 and 3 or b and c are executed only by subscriber T1. In fourth method step d, all subscribers T1-Tn involved in the method compute common key k according to the relation $k: = h(z1, g^{z2}, ..., g^{zn})$, it being required for (x1, x2, ..., xn) to be a function which is

symmetrical in arguments x2, ... xn. This variant drastically reduces the number of messages to be sent. An example of such a function g is, for instance,

$$k: = h(z1, g^{z2}, ..., g^{zn}) = g^{z1 \cdot z1} \cdot g^{z2 \cdot z1} \ldots \; g^{zn\, z1}.$$

[0027] The method according to the present invention can be advantageously used to generate a cryptographic key for a group of a several or at least three subscribers.

[0028] List of Reference Symbols

T1-Tn	subscribers 1 through n
Ti	undefined subscriber of T1-Tn
Tj	undefined subscriber of T1-Tn, different from Ti.
N	message
Ni	message of an undefined subscriber Ti
Mab	message of subscriber A to subscriber B
G	publicly known mathematical group
g	element of group G
p	large prime number
z	random number from the set (1,...p-2) selected via a random-number generator
k^{ij}; k^{1j}	common transmission key
k	common key
E(,)	algorithm
m	data record
f(x1,x2,...,xn)	function symmetrical in x1,x2,...,xn.
h(x1,x2,...,xn)	function symmetrical in arguments x2,...,xn.
A; B; C	designation of the subscribers in the exemplary embodiment

METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS

(2) What is claimed is:

1. A method for establishing a common key for a group of at least three subscribers, using a publicly known mathematical group G and a publicly known element of the group $g \in G$ of large order,

wherein

a) each subscriber (Ti) generates a message ($Ni = g^{zi} \bmod p$) from the publicly known element (g) of the group (G) and a random number (zi) selected or generated by him/her and sends it to all other subscribers (Tj),

b) each subscriber (Ti) generates a transmission key (k^{ij}) from the messages (Nj) received from the other subscribers (Tj, $j \neq i$) and his/her random number (zi) according to the function $k^{ij} := Nj^{zi} = (g^{zj})^{zi}$, the key being also known to subscriber (Tj) due to the equation $k^{ij} = k^{ji}$,

c) each subscriber (Ti) sends his/her random number (zi) to all other subscribers (Tj) in encrypted form by generating the message (Mij) according to $Mij := E(k^{ij}, zi)$, with $E(k^{ij}, zi)$ being a symmetrical encryption algorithm in which the data record (zi) is encrypted with the common transmission key (k^{ij}), and

d) the common key (k) to be established is determined by each subscriber (Ti) from his/her own random number (zi) and the random numbers (zj), $j \neq i$, received from the other subscribers according to the equation

$$k := f(z1, ..., zn),$$

it being required for f to be a symmetrical function which is invariant under the permutation of its arguments.

2. The method for establishing a common key as recited in Claim 1, wherein

a) all subscribers (Ti) involved in the method send the message ($Ni = g^{zi}$) they have generated to a subscriber such as the first subscriber (T1) who has previously been determined to carry out the subsequent method step,

b) the first subscriber (T1) encrypts the received messages (Nj) of the other subscribers (Tj, $j \neq 1$) for each subscriber (Tj) individually with his/her random number (z1) to form in each case one transmission key (k^{1j}), the key being also known to the subscriber (Tj) due to the equation $k^{1j} = k^{j1}$,

c) the first subscriber (T1) sends his/her random number (z1) to all other subscribers (Tj) in encrypted form by generating the message (M1j) according to M1j := $E(k^{1j}, z1)$, with $E(k^{1j}, z1)$ being a symmetrical encryption algorithm in which the data record (z1) is encrypted with the common transmission key (k^{1j}), and

d) the common key (k) to be established is determined by each subscriber (Ti) from the values (Ni) and (Nj), $j \neq i$, and the random number (z1) sent by the first subscriber (T1) in encrypted form with the aid of the equation

$$k: = h\,(z1, g^{z2}, ..., g^{zn}),$$

with h (x1, x2, ..., xn) being a function which is symmetrical in the arguments x2, ..., xn.

Abstract

The inventive method is based on a publicly known mathematical number group (G) and a higher order element of the group $g \in G$. In the first work step, a message corresponding to $Ni: = g^{zi} \bmod p)$ is sent by each subscriber (Ti) to all other subscribers (Tj), (zi) being a random number chosen from the set (1, ..., p-2) by a random number generator. In the second work step, each subscriber (Ti) selects a transmission key $kij: = (g^{zj})^{zi}$ for each other subscriber (Tj) from the received message (g^{zj}), with $i \neq j$, for transmitting their random number (zi) to the subscribers (Tj). In the third work step, the common key k is calculated as $k: = f(z1, z2, ..., zn)$ for each subscriber Ti. The inventive method can be advantageously used for generating a cryptographic key for a group of at least three subscribers.

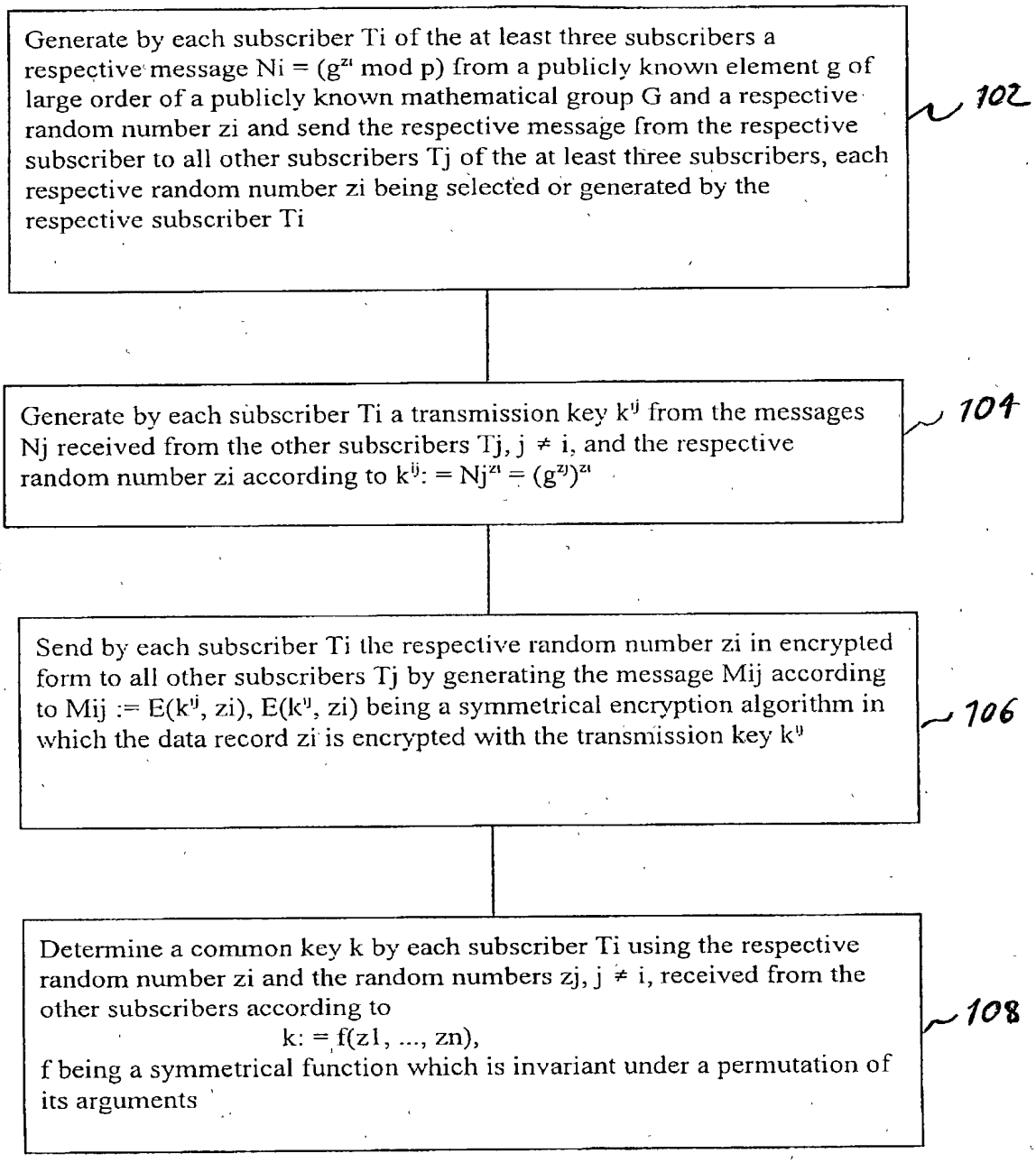

Generate by each subscriber Ti of the at least three subscribers a respective message Ni = (g^{zi} mod p) from a publicly known element g of large order of a publicly known mathematical group G and a respective random number zi and send the respective message from the respective subscriber to all other subscribers Tj of the at least three subscribers, each respective random number zi being selected or generated by the respective subscriber Ti
102
Generate by each subscriber Ti a transmission key k^{ij} from the messages Nj received from the other subscribers Tj, j ≠ i, and the respective random number zi according to k^{ij}: = Nj^{zi} = $(g^{zj})^{zi}$
104
Send by each subscriber Ti the respective random number zi in encrypted form to all other subscribers Tj by generating the message Mij according to Mij := E(k^{ij}, zi), E(k^{ij}, zi) being a symmetrical encryption algorithm in which the data record zi is encrypted with the transmission key k^{ij}
106
Determine a common key k by each subscriber Ti using the respective random number zi and the random numbers zj, j ≠ i, received from the other subscribers according to
k: = f(z1, ..., zn),
f being a symmetrical function which is invariant under a permutation of its arguments
108

FIG. 1

P99026US

DECLARATION AND POWER OF ATTORNEY

Docket No.:520:1007

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter that is claimed and for which a patent is sought on the invention entitled:

METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS,

the specification of which (check one)

☐ is attached hereto

☒ was filed on 10 July 2000 as International Application Serial No. PCT/EP00/06510 and was amended on (if applicable).

☒ I hereby authorize and request our attorneys, Davidson, Davidson & Kappel, LLC of 485 Seventh Avenue, New York, New York 10018 to insert here in parentheses (application number _____, filed _____) the filing date and application number of said application when known.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose all information that is known to me to be material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign and/or provisional application(s) for patent or inventor's certificate listed below and have also identified below any foreign and/or provisional application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

DE 199 38 198.4 Number	Germany Country	12 August 1999 Day/Month/Year Filed	Priority claimed ☒ Yes ☐ No
Number	Country	Day/Month/Year Filed	Priority claimed ☐ Yes ☐ No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial Number	Day/Month/Year Filed	Status
Application Serial Number	Day/Month/Year Filed	Status

And I hereby appoint Clifford M. Davidson, Reg. No. 32,728, Leslye B. Davidson, Reg. No. 38,854, Cary S. Kappel, Reg. No. 36,561, William C. Gehris, Reg. No. 38,156, Morey B. Wildes, Reg. No. 36,968, Robert J. Paradiso, Reg. No. 41,240, Erik R. Swanson, Reg. No. 40,833, Thomas P. Canty, Reg. No. 44,586, Livia S. Boyadjian, Reg. No. 34,781, and all other registered attorneys and agents at Davidson, Davidson & Kappel, LLC, U.S. Patent and Trademark Office Customer Number 23280, my attorneys, with full power of substitution and revocation, to prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected therewith; correspondence address: DAVIDSON, DAVIDSON & KAPPEL, LLC, 485 Seventh Avenue, 14th Floor, New York, New York 10018; Telephone: (212) 736-1940; Fax: (212) 736-2427.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, §1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first Inventor	Tobias MARTIN
Inventor's signature	
Date	
Residence	Rabenau, Germany
Post Office Address	Spitzengaerten 1 D-35466 Rabenau, Germany
Citizenship	German

Full name of additional Inventor	Ralf SCHAFFELHOFER
Inventor's signature	X
Date	X 02/14/02
Residence	Darmstadt, Germany
Post Office Address	Wittmannstr. 39 D-64285 Darmstadt, Germany
Citizenship	German

☒ Additional inventors named on attached sheet(s).

DECLARATION AND POWER OF ATTORNEY

P980265US

Docket No.:520.1007

As a below-named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter that is claimed and for which a patent is sought on the invention entitled:

METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS,

the specification of which (check one)

☐ is attached hereto

☒ was filed on 10 July 2000 as International Application Serial No. PCT/EP00/06510 and was amended on (if applicable).

☒ I hereby authorize and request our attorneys, Davidson, Davidson & Kappel, LLC of 485 Seventh Avenue, New York, New York 10018 to insert here in parentheses (application number 10/049,385, filed 02/11/2002) the filing date and application number of said application when known.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose all information that is known to me to be material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign and/or provisional application(s) for patent or inventor's certificate listed below and have also identified below any foreign and/or provisional application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

DE 199 38 198.4 Number	Germany Country	12 August 1999 Day/Month/Year Filed	Priority claimed ☒ Yes ☐ No
Number	Country	Day/Month/Year Filed	Priority claimed ☐ Yes ☐ No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial Number	Day/Month/Year Filed	Status
Application Serial Number	Day/Month/Year Filed	Status

And I hereby appoint Clifford M. Davidson, Reg. No. 32,728, Leslye B. Davidson, Reg. No. 38,854, Cary S. Kappel, Reg. No. 36,561, William C. Gehris, Reg. No. 38,156, Morey B. Wildes, Reg. No. 36,968, Robert J. Paradiso, Reg. No. 41,240, Erik R. Swanson, Reg. No. 40,833, Thomas P. Canty, Reg. No. 44,586, Livia S. Boyadjian, Reg. No. 34,781, and all other registered attorneys and agents at Davidson, Davidson & Kappel, LLC, U.S. Patent and Trademark Office Customer Number 23280, my attorneys, with full power of substitution and revocation, to prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected therewith; correspondence address: DAVIDSON, DAVIDSON & KAPPEL, LLC, 485 Seventh Avenue, 14th Floor, New York, New York 10018; Telephone: (212) 736-1940; Fax: (212) 736-2427.

(9)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, §1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first Inventor	Tobias MARTIN
Inventor's signature	X
Date	X 01/23/02
Residence	Rabenau, Germany DEX
Post Office Address	Spitzengaerten 1 D-35466 Rabenau, Germany
Citizenship	German

Full name of additional Inventor	Ralf SCHAFFELHOFER
Inventor's signature	
Date	
Residence	Darmstadt, Germany DEX
Post Office Address	Wittmannstr. 39 D-64285 Darmstadt, Germany
Citizenship	German

☒ Additional inventors named on attached sheet(s).

DECLARATION AND POWER OF ATTORNEY

Docket No.:520.1007

Full name of additional Inventor	Joerg SCHWENK
Inventor's signature	X
Date	X 26 January 2002
Residence	Dieburg, Germany
Post Office Address	Suedwestring 27 D-64807 Dieburg, Germany
Citizenship	German

Full name of additional Inventor	
Inventor's signature	
Date	
Residence	
Post Office Address	
Citizenship	

Full name of additional Inventor	
Inventor's signature	
Date	
Residence	
Post Office Address	
Citizenship	

Full name of additional Inventor	
Inventor's signature	
Date	
Residence	
Post Office Address	
Citizenship	

Full name of additional Inventor	
Inventor's signature	
Date	
Residence	
Post Office Address	
Citizenship	

Full name of additional Inventor	
Inventor's signature	
Date	
Residence	
Post Office Address	
Citizenship	

Full name of additional Inventor	
Inventor's signature	
Date	
Residence	
Post Office Address	
Citizenship	

Full name of additional Inventor	
Inventor's signature	
Date	
Residence	
Post Office Address	
Citizenship	